Articles

The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche

Denise Amram*

ABSTRACT

Starting from an analysis of the EU Reg. n. 2016/679 on General Data Protection Regulation (GDPR), the Author deals with the opportunity to translate the current strategies on Artificial Intelligence into a possible general risk-based framework that combines hard and soft law instruments with the practical needs emerging in different sectors where AI technologies find application (i.e. healthcare, industrial innovation and robotics, workplace, etc.). This analysis allows the Author to provide a notion of "AI Controller", whose main roles, responsibilities, and obligations are listed in a "General AI Regulation" proposal, illustrated in the last paragraphs.

* Dr. Denise Amram, Affiliate researcher at LIDER-Lab, DIRPOLIS Institute, Scuola Superiore Sant'Anna. This paper has been developed within the "SoBigData Plus Plus: European Integrated Infrastructure for Social Mining and Big Data Analytics" Project, funded by the EU Commission under the H2020 INFRAIA-1-2019 programme (GA 871042). I am grateful to the anonymous referees for their fruitful comments.

Keywords

GDPR – Accountability – Data Processing – Artificial Intelligence Regulation – AI Controller

Table of contents

1. Introduction

2. GDPR structure, principles, and notions

3. Is the GDPR structure suitable to frame the Artificial Intelligence regulatory model?
- **3.1.** Methods
- **3.2.** Required actions
- **3.3.** Goals

4. Beyond the principles and the legal obligations: room for contractual agreements

5. Towards an EU General Regulation on Artificial Intelligence?

6. Potentialities of the proposed model in light of extra-EU data protection law initiatives

7. Conclusive remarks

1. Introduction

Scientific progress opened new challenges in term of research and development thanks to the opportunity to process and exploit big amounts of data to automatically perform tasks, provide new solutions and predict unexplored scenarios. Technology innovation has become ubiquitous and pervasive with respect to the individual's daily routine. Therefore, a cultural change has progressively arisen, highlighting the value of personal information and their safe processing.

Considering that many tasks Artificial Intelligence systems may automatically perform are related either to data exploitation, or users' identification and tracking, including facial and voice recognition, or profiling and predict behaviours, personal data protection constitutes one of the main boundaries of the AI legal framework.

Accordingly, the EU General Data Protection Regulation n. 2016/679 (hereinafter "GDPR") provides a series of principles to enable personal data processing whose relevance goes beyond their strict field of application related to personal data processing. In a data-driven society a harmonised and binding regulation solely on a restricted category of data (like the personal ones) could be included as a possible scenario, but – as we will demonstrate

– it could also be taken into consideration as an effective model for further legislative initiatives[1].

This paper aims at analysing how the GDPR structure, principles, and obligations may not only be a necessary component but also inspire – *mutatis mutandis* – a possible EU General Regulation on Artificial Intelligence. Considering peculiarities and possible accommodation due to the widest field of application of AI technologies, such a general regulation should encompass not only personal data, but also structured as well as raw non-personal ones. New legislative initiatives, indeed, shall be tailored to protect fundamental rights both in case of human and artificial data processing, regardless the personal or non-personal nature of data. In fact, AI-based systems may affect individual and collective fundamental rights despite of the fact that analysis are performed through personal, pseudonymised, anonymised, or non-personal data.

In the following paragraphs, we will analyse GDPR principles, notions, and provisions that define the data protection by-design and by-default model, in order to extract possible legal concepts to set the AI compliance paradigm, to be developed considering the different nature, means, methodologies, and purposes of the data processing.

2. GDPR structure, principles, and notions

The GDPR has been introduced with the aim to both protect natural persons with regard to the processing of personal data and to ensuring the free movement of such data. From this perspective, the harmonization of the data protection legal framework within EU, that inspired many other extra-EU legislations[2], turned into a new ethical approach for a number of sectors[3].

The legislative technique consists of a series of 173 recitals that address the interpretation of the principles and obligations stated in the 99 articles divided into 9 chapters (princi-

[1] See the proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union 2017/228 that promotes the free movement of data within the EU, meaning for data "other than personal data as referred to in Article 4(1) of Regulation (EU) 2016/679".

[2] Data protection regulatory framework in a comparative perspective see R. Walters, L. Trakman, B. Zeller (eds.), *Data protection Law. A comparative analysis of Asia-Pacific and European Approaches* (Springer, 2019). Specific examples in the next paragraphs.

[3] Within the financial sector, see Franklin J., 'GDPR has kept AI ethical despite concerns' (2019), International Financial Law Review. October 2019: N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139213623&site=ehost-live. Accessed 17.6.2020; within the healthcare sector, Filippo Pesapane, Caterina Volonté, Marina Codari, et al. 'Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States' (2018), *Insights Imaging* 9, 745–753, https://doi.org/10.1007/s13244-018-0645-y; Chartrand G, Cheng PM, Vorontsov E *et al*, 'Deep learning: a primer for radiologists' (2017), *Radiographics* 37:2113–2131; Krittanawong C, Zhang H, Wang Z, Aydar M, Kitai T, 'Artificial intelligence in precision cardiovascular medicine' (2017), J Am Coll Cardiol 69:2657–2664; in the insurance sector see Guido d'Ippolito – Enzo Maria Incutti, 'I processi decisionali interamente automatizzati nel settore assicurativo' (2019) Rivista di diritto dell'impresa, 3, p. 735 ff., More in general, see Luciano Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Milano, 2017).

ples, rights of the data subjects, controllers and processors, transfers to third countries, independent supervisory authorities, cooperation and consistency, remedies, liability and penalties, provisions relating to specific processing situations), plus those chapters dedicated to general and final provisions, and to delegated and implementing acts.

In short, under the article 5 GDPR to process personal data in a lawful, fair, and transparent manner, the data controller shall implement technical and organizational measures to meet the purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality requirements[4]. In addition, she/he has to demonstrate to have met them (*i.e.* the principle of accountability puts the burden of proving compliance on data controllers).

A risk-based approach regulation[5], like the GDPR, combines hard law (obligations and enforcement tools, auditing, authorizations, report and monitoring, sanctions) and soft law instruments (opinions, standards, codes of conducts, self-regulation, binding corporate rules, …) in order to address compliance needs, considering priorities and urgencies. This approach allows a strategic efforts and resources allocation in light of the overall conditions of the obliged person – *rectius* the person who is responsible to mitigate and avoid risks determined by a given activity[6].

The risk-based approach of the GDPR identifies a series of obligations for the data controller all leading to a continuous assessment and monitoring of the personal data processing they enable. In the daily routine, this approach helps to follow a pre-determined standard check-list of activities to be performed in light of a tailored gap analysis performed by data controllers. Such a gap analysis aims to identify those measures that are appropriate to fulfil the obligations related to each and every unique characteristics of the personal data processing aimed at. This paradigm allows to protect data "by design" before enabling a data processing and "by default" within the given processing itself. Each data processing has to be analysed in order to tailor the compliance activity in light of its features[7].

Very often data flows – in this context we mean, in general, the processed information – encompass both personal and non-personal data. GDPR applies only to personal ones although it acknowledges at referral 26 that their borderlines are fluid. Accordingly, pseu-

[4] Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer, 2018).

[5] Malkom Sparrow, *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance* (Washington DC: Brookings Institutions Press, 2011).

[6] David Wright & Charles Raab (2014) Privacy principles, risks and harms, International Review of Law, Computers & Technology, 28:3, 277-298.

[7] Mary Donnelly and Maeve McDonagh, 'Health Research, Consent and the GDPR Exemption' (2019) 26 European journal of health law 97, see also Denise Amram, 'Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks' (2020) Computer Law & Sec. Rev. Vol: 37: 105413; G. Comandé. 'Ricerca in sanità e data protection un puzzle... risolvibile' (2019), *Rivista italiana di medicina legale e del diritto nel campo sanitario*, 188; See the Irish Data Protection Commission, *Guidance Note: Guidance on Anonymisation and Pseudonymisation*, June 2019.

donymised data (i.e. that information that can disclose one's identity only if associated to other ones) are included in its field of application[8].

Considering the broader category of personal data, their flows can be classified as general data-related or sensitive-data-related. The former ones refer to personal information that may identify data subjects, while the second ones refer to that information that may expose the data subject to a direct or an indirect discrimination. In particular, the latter may disclose racial or ethnic origins, political opinions, religious or philosophical beliefs, or trade union membership. The processing of genetic data, health-related data or sex life or sexual orientation are considered as particular category of data as well. Appropriate legal bases for data processing shall be identified respectively within article 6 GDPR for the general data (contractual relationship, legal obligation to be accomplished by the data controller, data subject's vital interest, public interest, legitimate interest of the data controller) and article 9 GDPR for the sensitive ones. The latter shall not be processed unless a specific legal basis has been identified. Article 9, para 2, *sub* a)-j) identifies the following legal conditions: data subject's explicit consent, legal obligation to be accomplished by the data controller, data subject's vital interest, legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, manifestly made public data, or to establish, exercise or defence within a legal claims, or for reasons of substantial public interest – within the purposes of preventive or occupational medicine – or for the assessment of the working capacity of the employee, or for medical diagnosis and health or social care, or to manage the related services, or the necessity for reasons of public interest in the area of public health, research and statistics purposes[9].

Considering who determines means and purposes of the data processing, flows can be governed by a single data controller, or by joint data controllers at the conditions agreed under article 26 GDPR, or on behalf of the data controller(s) by a data processor appointed under article 28 GDPR.

The illustrated classifications of data are functional to understand how the new cultural approach towards personal data protection could affect other legislative initiatives aimed at framing other potentially risky data-processing activities like the use of Artificial Intelligence (hereinafter also "AI"). In the next paragraphs, we will analyse possible accommodations to be addressed to the GDPR ecosystem in order to draft a regulatory framework for AI.

[8] Sophie Stalla-Bourdillon – Alison Knight 'Anonymous Data v. Personal Data – False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016-2017) 34 Wis. Int'l L.J. 284.

[9] See Giusella Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla privacy e sulal protezione dei dati personali* (Zanichelli, 2017); Vincenzo Cuffaro, Roberto D'Orazio, Vincenzo Ricciuto, *I dati personali nel diritto europeo* (Giappichelli, 2019); Giovanni Comandé- Gianclaudio Malgieri (eds.), *Guida al trattamento e alla sicurezza dei dati personali* (IlSole-24Ore, 2019).

3. Is the GDPR structure suitable to frame the Artificial Intelligence regulatory model?

The last decade has been identified as the "big data era", where Artificial Intelligence techniques provide the opportunity to process huge amount of structured and unstructured data and to develop and share high speed and high level performance applications within the Internet of Things has driven a revolution of the way of thinking and producing, affecting all sectors from economics and finance, to industrial, agriculture, healthcare, education etc[10]. For Artificial Intelligence, that is not uniquely defined[11], we consider those "*systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals*"[12], through "*the reproduction of human cognitive functions such as problem solving, reasoning, understanding, recognition, etc. by artificial means, specifically by computer*"[13], or by systems "*that mimic cognitive functions, such as learning and problem-solving*"[14]. A horizontal and a vertical dimension has been identified to distinguish AI excellence in performing a task from the versatile human intelligence[15].

In this context, despite of the recognition of the rights to privacy[16] and data protection within the international conventions, national constitutions and *ad hoc* legal frameworks, the legislative process is a step behind the development of AI-based systems[17].

[10] See Seamans, recalling several reports from stakeholders and economic operators, like Accenture, McKinsey Global Institute, World Economic Forum, see Robert Seamans, 'Artificial Intelligence and Big Data: Good for Innovation?', *Forbes* (Sept. 7th 2017), https://www.forbes.com/sites/washingtonbytes/2017/09/07/artificial-intelligence-and-big-data-good-for-innovation/#1409eb5f4ddb. Accessed on 21.06.2020; Viktor Mayer- Schönberger – Kenneth Cukier, *Big data: a revolution that will transform how we live, work, and think* (John Murray Publishers, London, 2013). See OECD, Report on 'Data-driven innovation. Big Data for Growth and Well-Being', 2016, http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm, accessed on 22.6.2020

[11] Miriam C. Buite, 'Towards Intelligent Regulation of Artificial' (2019), *European Journal of Risk Regulation*, 10(1), 41 ff, 43.

[12] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM (2018) 237 final.

[13] K. K. Ogilvie and A. Eggleton, Challenge Ahead: Integrating Robotics Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare Systems (2017), 5, https://sencanada.ca/content/sen/committee/421/SOCI/reports/RoboticsAI3DFinal_Web_e.pdf, accessed on 22.6.2020.

[14] Russell S, Bohannon J, *Artificial intelligence. Fears of an AI pioneer* (2015), Science 349:252.

[15] Giovanni Comandé, 'Multilayered (Accountable) Liability for Artificial Intelligence', in Sebastian Lohsse - Reiner Schulze - Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Hart Nomos, 2018) 165ff, 167.

[16] Among others, see Article 12 of the Universal Declaration of Human Rights, 1948, article 17 of the International Covenant on Civil and Political Rights, 1966; article 16 of the Convention on the Protection of all Migrant workers and members of their families, 1990; article 8 of the European Convention on Human Rights, and article 11 of the American Convention on Human Rights, 1969; and the article 18 of the Cairo Declaration of Human Rights in Islam, 1990; articles 16 and 21 of the Arab Charter on Human Rights, 1994; and article 19 of the African Charter on the Rights and Welfare of the Child.

[17] For a comparative analysis between GDPR and data protection regulations in the United States considering the life cycle of personal data addressing possible issues within an AI system, see John Frank Weaver, 'Artificial Intelligence and Governing the Life Cycle of Personal Data' (2018) 24 Rich JL & Tech 1.

To pretend that AI regulation challenges are satisfied by regulating data protection and privacy rights can work within the rhetoric figure of the "synecdoche", where a part stands for the whole. In this context, however, the potentialities of the GDPR shall boost a coherent protection of the "other" fundamental rights involved within the massive development of AI technologies within the current societal context. A number of soft law initiatives, in fact, identified some pillars to address a possible regulatory framework of the Artificial Intelligence paradigm, including lawfulness, ethics, and robustness[18].

Lawfulness could be met only if all legal requirements are filled (and not only the ones emerging from the data protection legislation): this is particularly complicated as an organic regulation has not been enacted yet. Nevertheless, the EU Commission is focusing on the impact of AI systems on fundamental rights, launching a strategy aimed at achieving both excellence and trust within the development.

According to the White Paper on Artificial Intelligence – A European Approach to Excellence and Trust[19], in fact, the use of AI "*entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes*". Fairness, indeed, is achievable whereas such risks are avoided. Although a complex and fragmented framework applicable to AI might derive from a recognition of technical standards, binding rules applicable to specific fields, and soft law regulations, a general, coherent, and widely applicable one has become not only a priority, but also an urgent action, as AI-based services and products are already part of our daily routine.

The structure of the GDPR may influence the new legislative process as well. To analyse principles stated in the GDPR and extend their possible efficacy specifically to a AI regulation is a first exercise to assess the legislative model in terms of suitability in order to identify boundaries and frontiers of what lawfulness means for the AI context[20].

To this end, a regulatory framework on AI shall adopt a risk-based approach to assess, and therefore accept, for each AI application, a solution/model/implementation in light of a check and balances system of hard law and soft law instruments.

From this perspective, the High-Level Expert Group on AI within the Ethics Guidelines for Trustworthy Artificial Intelligence presented in April 2019 at the EU Commission an extended notion of AI systems including software and hardware "*designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured*

[18] See the Working Party Article 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, last access 21.06.2020, recalling notions, legal bases, and principles for profiling and automated decision-making.

[19] *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[20] Celine Castets-Renard, 'Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making' (2019) 30 Fordham Intell Prop Media & Ent LJ 91.

data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal", distinguishing machine learning techniques, machine reasoning, and robotics applications[21].
Starting from this wide definition, since the AI system is designed by humans, the first step consists of identifying who shall be responsible, accountable, and liable to assess risks that may occur in the given application, monitoring the development, and comply with the regulatory framework according to the current standards and scientific knowledge. As above-stated, the GDPR paradigm assigns obligations to the one who determines means and purposes of the personal data processing. Within the AI context, we shall identify the *mutatis mutandis* "AI controller".
For the development of the AI system, the algorithm control consists of *methods for data acquisition* (*i.e.* what function/algorithm is chosen and which data train the algorithm), *actions required* (*i.e.* what task shall the AI perform), and *goals* (*i.e.* which is the final purpose of the automated decision making/reasoning activity)[22]. Therefore, the "AI controller" could be the one who determines methods, actions, and goals of a given AI-based system.
In addition, a series of roles could be identified to support the AI controller in the assessment and monitoring activities: likewise the GDPR, an internal distribution of roles and responsibilities, a so-called RACI matrix – that identifies who is Responsible, Accountable, Consultable, and Informed of the AI processing – may offer a best practice to follow (and perhaps to make it as a binding provision) to better distinguish and trace human choices and interventions on the development and use of AI technologies.
A second regulatory step may refer to the opportunity to identify rules addressing the AI external governance in order to verify case-by-case conditions to share responsibilities within the development and the use of technology. For instance, to consider whether or not (and how) more than one controller is involved in determining methods, actions, and goals[23].

3.1. Methods.

Methods generally refer to "algorithms libraries" that define functions for a variety of goals, operating on ranges of elements. They are therefore comparable to the materials used in a given supply chain.
In this perspective, several scenarios might be identified considering different grounds of control within the choice (terms of application are the ones emerging in the source; the

[21] *Ethics Guidelines for trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[22] Enza Pellecchia, 'Profilazione e decisioni autmatizzate al tempo della *black box socieety*: qualità dei dati e l leggibilità dell'algoritmo nella cornice della *responsibile research and innovation*', *Nuova giur. civ. comm.*, 2018, p. 1209 ff.

[23] On the human control on algorithms, see Stefano Rodotà, *Il mondo in rete* (Roma-Bari, 2017), Remo Bodei, *Dominio e sottomissione. Schiavi, animali, macchine e l'intelligenza artificiale* (Bologna, 2019), and Giuseppe Zaccaria, 'Figure del giudicare: calcolabilità, precedenti, decisione robotica' (2020), *Riv. Dir. Civ.*, 277 ff.

use of that specific algorithm is – or is not – included in the ones that are meant for it; the use of that specific algorithm is timely applied or obsolete), recalling notions developed in the context of the so-called Consumer[24] and General Product Safety Directives[25] and related national implementations.

Methods consist also of the activities related to data acquisition: which dataset shall train the algorithm, under the premise that "*data accuracy and relevance is essential to ensure that AI based systems and products take the decisions as intended by the producer*"[26]. At this stage, an overlap /correspondence accommodation between "AI controller" and "data controller" under GDPR is unavoidable whereas the AI system processes personal data. In this perspective, the pillars of personal data protection shall be taken into consideration and further room of accommodation shall be investigated.

In particular, the principle of data minimization, that is applicable for personal data seems to not properly fit with the aims of the AI systems development, where algorithms become more accurate with the largest amount of data processed. Therefore, a legislative initiative on AI shall introduce provisions aimed at identifying actions to properly select datasets for data acquisition as well as applicable technical standards and organizational measures to ensuring that the developer will responsibly train the chosen algorithm. In this regard, a testing/validation of outcomes shall be performed by the AI controller in order to assess whether or not the data acquisition and exploitation ensure the accurate and predicted results.

To this end, a possible collaboration between the AI controller and the data protection officer as well as the identification of "AI officer/advisor", possibly with an interdisciplinary background for the purposes that we will further illustrate, could be a fruitful support to address compliant choices, also in terms of "consultable" and "responsible" roles, within the above-mentioned RACI matrix.

In this step, artificial intelligence is fully controlled by human behaviours: therefore, the GDPR structure of rights and duties and the general enforcement paradigm emerging from the accountability principle (*i.e.* the burden of the proof to have accomplished is on the data controller) appears suitable, with all the consequences in terms of liability rules and insurable risks.

[24] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[25] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

[26] White Paper on On Artificial Intelligence – A European approach to excellence and trust. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en, p. 8.

3.2. Required actions

To determine the "required actions" is paramount in terms of fairness, transparency, and lawfulness. Tasks shall be entailed within legal basis and be explainable to the scientific community, in order to guarantee technical standards of safety and performance and, at the same time, it shall be explainable to the data subject, in case the automated decision making individually impacts on her/his rights.

In other words, regulation shall include black box as well as white box scenarios. For example, automated "sensitive" data profiling will be approved if it comes with a so-called "white box", where the way of profiling is understandable. By opposition, the so called "black box", where the profiling is not understandable, shall be duly regulated as it may present more problematic effects[27]. This principle emerges already from article 22 GDPR on automated decision-making producing legal effects on the individual person[28].

Within this context, the relationship between artificial intelligence and human intelligence is double. Actions are determined by the "AI controller", but the results of the processing may affect other subjects, namely the data subjects or final users, whose fundamental rights shall in any case be protected and enhanced by the AI application[29].

Therefore, this step shall be regulated both in terms of ethical and legal compliance, as the developer has to proactively assess possible direct and indirect risks on human beings caused by the AI processing. Again, at this stage, the developer shall be accountable as she/he has to demonstrate to have considered and assessed any risks connected to the use of AI, also during a testing/validating step of the developed technology[30].

A RACI matrix is particularly effective if we consider that different expertise shall establish a unique dialogue to fully assess, test, validate, and responsibly internally approve a given AI-system, despite of the external controls that a given sector may introduce to allow the exploitation of the possible innovative outcome.

[27] Mélanie Bourassa Forcier, Hortense Gallois, Siobhan Mullan, Yann Joly, 'Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?' J Law Biosci. 2019 Oct; 6(1): 317–335; Mike Ananny – Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability', New Media & Soc'Y 973, 980 (2016).

[28] Giovanni Comandé, 'The Rotting Meat Error: From Galileo to Aristotle in Data Mining?' (2018), *European Data Protection Law*, 270 ff, Margot E. Kaminski – Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations' (2019) U of Colorado Law Legal Studies Research Paper No. 19-28. Available at SSRN: https://ssrn.com/abstract=3456224 or http://dx.doi.org/10.2139/ssrn.3456224

[29] Celine Castets-Renard, 'Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making' (2019) 30 Fordham Intell Prop Media & Ent LJ 91.

[30] See the proposal of Human Rights Impact Assessment Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in Wright and De Hert (n 21), 33-76; James Harrison, and Mary-Ann Stephenson, 'Human Rights Impact Assessment: Review of Practice and Guidance for Future Assessments' (Scottish Human Rights Commission, 2010) http://fian-ch.org/content/uploads/HRIA-Review-of-Practice-and-Guidance-for-Future-Assessments.pdf , and its variation oriented to social profiles as well, namely the Human Rights, Ethical and Social Impact Assessment (HRESIA) proposed by Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', 34 Comp. L. & Sec. Rev. 754 (2018).

This is particularly true, for example, where the AI controller appoints (or he/she has asked a third party) to develop an AI based system for a field that needs specific requirements. This could be the case of an AI-based tool for medical devices[31] where computer science skills shall understand needs and values of healthcare sector and protect data subjects not only from possible attempts to their personal data and privacy, but also their health, and sometimes to the private life of their family members, or their work. Same issues emerge for robotics applications that may be added in a supply chain to support the human-activities: fundamental rights to be protected are not only related to personal data and privacy, but also to freely express opinions, work-life, health, etc.
For these reasons, the above-mentioned White Paper has identified few grounds of assessment for AI technology in order reach the excellence and trustworthy target.

– *Human agency and oversight*: human intelligence shall always maintain the control on artificial intelligence. Therefore, actions shall be oriented towards a specific goal and limited to it, as for each combination of methods, tasks, and goals a given assessment shall be performed by the AI controller. In this perspective, auditing activities could be established in order to make a procedure of external and independent check.

– *Technical robustness and safety*: the AI system shall follow the highest standards and requirements developed by the competent agencies and bodies. In this regard, the ENISA (the European Union Agency for Cybersecurity) and ISO/IECJTC 1/SC 42 are providing standardization in the area of Artificial Intelligence in order to build up a robust and technically safe ecosystem, defining technical specifications to be followed. In terms of the principle of accountability, the developer could be asked to demonstrate to have followed the current technical standards and to justify his/her choices.

– *Privacy and data governance*: as above-stated, this part shall not only recall and be compliant with the GDPR, but it has to be the opportunity to introduce specific obligations to verify the alignment of procedures, responsibilities, and obligations. In particular, the data protection impact assessment under article 35 GDPR shall be synergically embedded in the AI impact assessment as a specific ground of evaluation of

[31] The EU Regulation 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (hereinafter "MDR") provides a series of obligations for the manufacturer, including the appointment of a (or more) person(s) responsible for regulatory compliance under article 15 to ensuring the conformity and the quality of devices, monitoring the technical documentation, fulfilling the post-market compliance obligations, issuing the due reports, and accomplishing the provisions for clinical investigations, entering into force in 2021. See Brian Daigle and Mihir Torsekar, 'The EU Medical Device Regulation and the U.S. Medical Device Industry' (2019) 2019 J Int'l Com & Econ 1 and Cesare Bartolini – Gabriele Lenzini, 'Sistemi medici e conformità legale' (2019) Riv. It. Med. Leg., 225 ff.

the system[32]. Accordingly, a new regulation could identify a provision where the "AI controller" has to collect and demonstrate GDPR compliance, whereas personal data are processed, identifying possible scenarios: i) if the "AI controller" is the same person/body of the data controller, then the AI controller shall directly deal with the GDPR compliance; ii) if the "AI controller" is only a "data processor" of a personal data flows, before collecting personal data to be processed by the AI, she/he shall be appointed as data processor under article 28 GDPR. This could be the case of an agreement where the data controller asks a R&D company to provide an automated tool to automatize a given process starting from a database structured by the same data controller; iii) if the "AI controller" acts also as a joint controller of the personal data flows, an agreement under article 26 GDPR shall be drafted. This could happen between partners that share different datasets and only one of them trains an algorithm.

– *Transparency*: within the GDPR this principle is mainly accomplished through the information sheet that informs the data subject about the privacy governance, including contacts of the data controller and data protection officer, type of data processed, means, purposes and legal basis, recipients, duration and possible data retention, possible re-use policy, and overall which rights can be enforced and how. Transparency is also relevant within a data breach procedure as in case of notification to the data protection authority, the lack of information to data subject shall be expressly justified. Article 22 GDPR adds something more as it requires a specific legal basis to allow an automated decision-making directly producing legal effects on data subjects (contractual relationship, legitimate interests, expressly given consent), introducing a substantial provision in case of personal data acquisition and collection to be applied to an AI-based system. The formula is expressed through a negative statement that allows data subjects to access to a regime of opposition, consisting of the right to obtain a human intervention, express point of views, contest the outcome of the automated decision making. These rights shall find a proper field of application within the AI regulation, identifying conditions to be applied also whereas non-personal data are used, in order to maintain the human-centric approach towards the AI.

– *Diversity, non-discrimination, and fairness*: these principles refer to possible bias that the AI system may incur or produce while processing data and reproducing results in the decision-making or within the final tasks. In order to avoid them, beyond the proof to have followed specific technical standards, a validation step aimed at testing the results under the possible ground of discrimination shall be provided before approving

[32] Charles D. Raab, 'Information privacy, impact assessment, and the place of ethics' (2020), Computer Law & Security Review, 37, 105404 and previously, Colin J. Bennett, Charles C. Raab, 'Revisiting the governance of privacy: contemporary policy instruments in global perspective' (2018) Regulation a& Governance, 14, 3.

the developed technology. However, a couple of difficulties may arise. Firstly, this step includes a strong interdisciplinary evaluation, not always familial for the AI developers. Secondly, a double ground of analysis shall be provided: a first assessment on possible attempts to diversity, non-discrimination, and fairness can address the development strategy towards a peculiar activity of data pooling as a technical measure to mitigate risks of biases. Then, a second evaluation on unpredictable risks and attempts emerging from the results shall be performed, as biases have mostly been discovered *ex post* (like the well-known case of Google Photos where the annotation algorithm had identified black people like gorillas)[33]. The "AI officer" may support the "AI controller" in this activity of test and validation: a deep knowledge and sensitive attitude towards inclusiveness and fundamental rights shall become the key-skill to turn a biased algorithm to a trustworthy and excellent one. Paths to strengthen the efficacy of these provisions could be encouraged by institutions and economic operators in terms of accountability.

– *Societal and environmental wellbeing*: as a consequence of the illustrated challenges, the AI regulation shall encourage the societal and environmental wellbeing, by providing possible incentives in developing specific sectors: awareness and positive actions against the digital divide shall be promoted. To answer this challenge the legislative initiative may encourage the adherence to codes of conducts and certification mechanisms aimed at addressing compliance on the accountability ground.

The legal challenge is to develop a framework able to identify those measures that allow the AI controller to meet a by design and by default compliance as well as boundaries for an enforceable accountable behaviour.

3.3. Goals

Goals refer to the main purposes defined by the AI controller. In this part, a general regulation shall maintain the opportunity for national legislators to implement possible safeguards and national accommodation considering that AI could be applied to several sectors, governed by national legal frameworks, where the introduction/application of new systems based on machine learning, deep learning, automated decision-making may need to re-frame or amend specific provisions to allow a full harmonization with the EU paradigm.

For instance, if we consider the healthcare system[34], the development of solutions that can support the early-detection, diagnosis, and treatment are affecting both the services organization and the clinician-patient relationships. Therefore, the compliance activity

[33] Aylin Caliskan, Joanna J. Bryson, Arvind Narayanan, 'Semantics derived automatically from language corpora contain human-like biases' (2017), Science: Vol. 356, Issue 6334, pp. 183-186, DOI: 10.1126/science.aal4230.

[34] Tokio Matsuzaki, 'Ethical Issues of Artificial Intelligence in Medicine' (2018) 55 Cal W L Rev 255.

related to the above-mentioned grounds could be adapted to the specific needs and constrains emerging from the different national health protection paradigms. In this case a double assessment – one for the development and another one for its placement in the market – shall be performed as well. The introduction of the ethical-legal assessment is more immediate for the AI-applications within the healthcare system, as the impact of research activities on fundamental rights usually needs the involvement of competent ethics committees. According to the Declaration of Helsinki medical research, in fact, is subject to the definition of a protocol that shall be drafted and submitted for approval. It has to illustrate the background and rationale, purposes and activities, benefits and risks, developing the information sheet, and the informed consent template, including the privacy policy, according to the applicable national legal framework[35]. Innovation and research in clinical and medical sectors are usually subjected to follow the principles and protocols developed within the scientific community. A risk-based approach is also applied to allow the diffusion of a new medical device, treatment, pharmaceutical product and a series of national and international authorizations have to be obtained for the pre-trials and trials before placing it within the market. The use of AI-technologies becomes an element of evaluation by the competent ethical committees.

A different approach could be applied in case of robotics applications or digital twin: both domains are regulated only in terms of ISO safety and technological standards, and not addressed in terms of binding regulation neither for their physiological development nor in case of accidents or misuse. From this perspective, the interaction between the use of AI systems and the Internet of Things (IoT) environment shall be taken into consideration as a possible scenario to be regulated beyond the technical standards followed to put the final product into the market as a certified one. An AI regulation shall cover this scenario from a top-down level, able to combine different issues.

From this perspective, considering the massive use of AI systems, a regulatory framework shall establish possibly independent authorities and bodies. This shall support the existing ones in the assessment and evaluation of the AI-based applications in the given sectors (like the ethics committees for clinical trials that have to deal with AI-systems, or data protection authorities, or competition committees, or bodies to protect vulnerable groups, or animals wellbeing, etc.). Otherwise, it could be appropriate to identify centralized – at least at EU level – mechanisms of preventive as well as of assessment/consultation as a pre-requirement to access the sectorial/specific procedures of authorization/approval from the decentralized competent body. Also on this field, the GDPR experience on the Euro-

[35] L. Williatte-Pellitteri, 'New Technologies, Telemedicine, eHealth, Data...What Are You Talking About? The Lawyer's Point of View', in A. André (ed), *Digital Medicine* (Springer, Cham, 2019) 93; Nathan Cortez, 'The Evolving Law and Ethics of Digital Health', in Homero Rivas – Katarzyna Wac (eds.), *Digital Health Scaling Healthcare to the World* (Springer, Cham, p. 249 ff; Denise Amram, 'L'Ulisse accountable. Ricerca e protezione dei dati concernenti la salute: il tentativo di armonizzazione al livello europeo post GDPR e le interpretazioni offerte dai sistemi irlandese, belga, spagnolo e italiano' (2019), *Rivista Italiana di Medicina Legale e del Diritto nel campo sanitario*, 209 ff.

pean Data Protection Supervisor and national data protection authorities as well as the European Data Protection Board and the mechanism of prior consultation under article 36 GDPR can offer, at least at organizational level, an efficient model to be pursued.

4. Beyond the principles and the legal obligations: room for contractual agreements

Once that we have identified what is meant for AI, which could be the principles and main roles to be regulated, and the relationship between soft law and hard law tools, we may consider the boundaries of the legislative activity in reference to the contractual autonomy of the main players, namely the AI controller and data subjects (or end-users, addressees). In particular, looking at the GDPR structure once again, and to its multilevel system of check and balance, contractual autonomy could govern some aspects of the AI technology development as well[36].

First of all, the profiles related to the data protection agreements under the mentioned articles 26 and 28 GDPR in case of personal data. Secondly, issues related to the ownership of the collected data. Thirdly, the protection of intellectual property rights of the final output. To avoid disputes the AI regulation may standardize some notions and address possible binding content to be included in these agreements, especially oriented to guarantee the exercise of data subjects' rights[37].

Another contractual issue that could be included is the identification of insurable risks to better protect data subjects from possible bias (in case that one of the algorithm fails on one of the ethical profiles, or for undesired outcomes during the test phase), or errors (like the false or over and/or under prediction for a future event), or reputational ones[38]. Furthermore, the occurrence of external threats like cyberattacks to the system or misuse of the outcome shall be made subject to compulsory insurable. In fact, this would establish a fairer equilibrium to ensuring damage compensation to the data subject/addressee/end-user for those risks that are more severe or frequent[39].

[36] See Zeno-Zencovich remarks on who owns big data and the relative consequences on contractual clauses on personal data and data access: Vincenzo Zeno-Zencovich, 'Ten legal perspectives on the "era of big data revolution" (2016), *Concorrenza e mercato,* 29 ff., see remarks on law-making by Roberto Pardolesi – Antonio Davola, 'Algorithmic legal decision making: la fine del mondo (del diritto) o il paese delle meraviglie' (2020), *Questione Giustizia*, 1, 104 ff. at 110.

[37] Michael Mattioli, 'Disclosing Big Data' (2014), Minn. L. Rev., 99, 535 ff; W. Nicholson Price II, 'Big Data, Patents, and the Future of Medicine' (2016) Cardozo L. Rev., 37, 1401 ff.

[38] See Sonia K Katyal, 'Private Accountability in the Age of Artificial Intelligence' (2019) 66 UCLA L Rev 54.

[39] See the Expert Group on Liability and New Technologies – New Technologies Formation, 'Liability for Artificial Intelligence and Other Emerging Digital Technologies', https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608, last access 23.06.2020, also recalling the principles stated in Article 15:101 of the Principles of European Insurance Contract Law (PEICL).

5. Towards an EU General Regulation on Artificial Intelligence?

This paper has shortly illustrated the potentialities of the GDPR regulation as model in order to propose a possible more extensive normative system for Artificial Intelligence, whose peculiarities and challenges have been addressed pragmatically taking into consideration both current soft law initiatives and the identified pillars towards a trustworthy and excellent AI for Europe.

To sum up our remarks, we propose how to address some contents for a General AI Regulation, according to a risk-based oriented system of check and balance aimed at ensuring the development of any AI-systems in light of the applicable principles. The Regulation shall consider the peculiarities emerging within the different sectors and therefore provide the opportunity for each AI controller to establish within his/her organization a RACI matrix to allocate tasks, roles, and responsibilities. Under this system, independent authorities shall provide assistance, consultancy and incentives to develop awareness and trustworthiness among data subjects/end-users/stakeholders as well as to promote possible interdisciplinary skills development aimed at facilitating the internal assessment activities and boost the cultural and inclusive challenge that the AI is driving. Below a tentative table of contents:

A. Principles and definitions.

Principles and definitions shall provide a short overview of the main pillars of the AI regulatory framework, identifying what is meant for the following legal and technical concepts: Fundamental rights (Human Dignity, Health, Data protection and privacy (and the ones stated under article 5 GDPR); Technical Safety and Robustness; Ethical-legal by design and by default; Accountability; Artificial Intelligence; Methods, Required Actions, and Goals of the AI System; AI governance and RACI matrix; AI controller, AI joint controllers, and AI processor.

B. General obligations.

General obligations shall be addressed to the defined steps of the AI system development: Methods, Required Actions, and Goals. It shall also reflect the risk-based approach: all the provisions shall be functional to perform a continuous impact assessment of the design, development, and validation steps. Therefore, it shall include records of the technical specifications for the designed application, the list of the applied technical standards, the results of a comparative assessment of the possible applicable methods, a list of designed actions and predictable ones, goals pursued with the development of the given AI tool, a list of the involved fundamental rights affected by the AI system, an ethics assessment[40]

[40] See the interesting proposal of algorithmic DPIA in Kaminski - Malgieri, *cit.*, 25 ff., on the way of Reuben Binns, 'Data protection impact assessments: a meta regulatory approach' (2017) 7 Int'l. Data Priv. L. 22.

under them in terms of risks and benefits as well as the organisational and technical measures to be implemented, a data protection impact assessment under article 35 GDPR (if applicable), a list of possible end-users including measures to mitigate possible digital divide or boost awareness.

This part shall also identify the organizational measures to allocate roles and responsibilities, including: a RACI matrix identification and governance (*e.g.* relationships between data protection officer, AI officer, system administrator, security manager, AI manager, and AI controller), conditions to sign data protection and/or ownership agreements, possible binding contents to better achieve the trustworthy and excellence purposes, and to avoid disputes/pre-determine responsibilities in case of mistakes/errors/bias/damages, possible enforcing tools (*i.e.* the *astreinte* in case of delay in submitting authorizations/application for ethics approvals, or in case of defaulting collaboration etc.), terms and conditions to avoid/submit for application for authorizations and approvals from ethics committees and/or competent bodies (for pre-trials, trials, and validation of the AI-based product/service).

Technical measures: technical standards requirements and procedures to reach acceptable levels of robustness (including trade and certification procedures, ISO norms, auditing activities, and incentives for training) both of the AI developed system and the whole IoT ecosystem interacting with it.

Data subjects, stakeholders, and end-users' rights: requirements to be included in the information, clauses stated in the terms and conditions of the AI-system, identification technical and organizational measures to mitigate vulnerabilities, possible assessment activities to be performed in order to make the given AI-system interoperable and interactive with other ones in a complex smart solution.

C. Specific obligations for AI tools in the Healthcare Sector.

This section shall be coherent with the regulatory frameworks on Medical Device Regulation (Medical Device Regulation, EU Reg. n. 745/2017), Clinical Trials Regulation (Clinical Trials Regulation, EU Reg. n. 536/2014), and the European regulatory system for medicines, including the related procedures emerging from the given sector also at national level.

As above-illustrated, AI-systems that either process health-data or support clinical decisions have a significant impact on individual and collective fundamental rights both in a patient-oriented perspective and in a professionals' one. From this perspective, the regulatory framework aimed at identifying the compliance activity shapes new frontiers of the Health Technology Assessment[41], providing the most sustainable and efficient solution for

[41] Mark L. Flear, Anne-Maree Farrel, Tamara K. Harvey, Thérèse Murphy, *European Law and New Health Technologies* (Oxford, 2013), see also Leopoldo Trieste et al., 'Razionale e strumenti della valutazione economica in sanità', in G. Carnevale, P. Manzi (eds), *Manuale di governance sanitaria* (PM edizioni, 2017), 427 ff.

the development of services and products in the healthcare sector *by design* (during its development) and *by default* (in terms of acceptability, usability, and market placement)[42]. Measures to ensuring a massive data training could be required before allowing a concrete support of AI tools within the clinical decision making[43].

D. Specific obligations for AI tools in the workplace.

This section shall embed principles stated within the workplace safety regulations and non-discrimination directives as well as provide consistency mechanisms of national agreements and protocols to be agreed with the workers representations and trade unions.
It shall promote, in particular, an assessment of the introduction of AI tools to develop new skills and expertise related to the automated-support in the workload, designing specific paths to facilitate the digitalisation of services and supply chain boosting the individual and collective acceptability.

E. Specific obligations for AI-system for industrial innovation and robotics (including obligations for human-robot interactions).

This section shall provide specific obligations in order to enhance the principles stated within the *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, addressing the adherence to mechanisms aimed at continuously performing the assessment of the related deep learning features of the AI-systems once the innovation has been placed in the market[44]. A system to provide alerts, or develop awareness for stakeholders and end-users in the market shall be considered and expressed in terms of follow-up monitoring, that could be promoted through self-regulation mechanisms (codes of conducts, trades, and certifications)[45] or it could be attributed to external boards (like consumers associations) or independent authorities (for example, the opportunity to maintain a registry on approved AI-tools, linked to insurance renewal or taxes purposes whether applicable to the specific innovation).

[42] WHO, *2015 Global Survey on Health Technology Assessment by National Authorities*, World Health Organization 2015 and the Strategy for EU cooperation on Health Technology Assessment (HTA) adopted by the HTA Network in Rome on 29.10.2014.

[43] Andrew L Beam – Isaac S. Kohane, 'Big Data and Machine Learning in Health Care' (2018) 319 JAMA 1317. An attempt to identify an ethical path for AI in healthcare is proposed by Tokio Matsuzaki, 'Ethical Issues of Artificial Intelligence in Medicine' (2018) 55 Cal W L Rev 255: 272-273.

[44] Yann LeCun et al., 'Deep Learning' (2015) 521 Nature 436.

[45] Article 40 GDPR introduces the opportunity to approve Codes of Conduct at EU level, providing a de facto self-regulation tool with an extensive effectiveness, see Franco Pizzetti, 'GDPR e Intelligenza Artifciale Codici di condotta, certifcazioni, sigilli, marchi e altri poteri di sot la previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA', in A. Mantelero – D. Poletti (eds), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa University Press, 2018) 69 ff, 93.

As far as human-interaction is concerned, a truly human-centric approach shall also analyse the impact of such an interaction has on the daily-routine in light of the values shared in a given historical eve. For example, the possibility to interact with an avatar[46] or with a robot may support a workload in a supply chain, better train some professional skills, but it can also reduce the distress or trauma related to the bereavement damage. The psychological implications of dual-twin environments are a challenge that shall be addressed as well: avatars may be used to cover the concepts of presence/absence, support some process, but they can also emphasize some human vulnerabilities. This kind of consequences need a deep assessment both at individual level and collective one.

F. Specific obligations for AI tools addressed to vulnerable individuals or groups.
AI-tools and systems shall take into consideration the vulnerabilities of the end-users, in order to reduce the digital divide, not to create disadvantages for individuals or group of individuals. However, it is possible that the analysis of information related to some vulnerabilities could be the main task of the developed technology, in order to provide a technological support for a given service or product. In this case, a specific obligation to not misuse the outputs of the tool shall be provided together with specific policy related the re-use or sharing of methods, actions, purposes and, of course, data.

G. Independent authorities and supervisors.
Independent body and authorities aimed at monitoring, standardizing, controlling, sharing awareness and training on AI systems shall be established. Furthermore, this section shall rely with possible mechanisms and relationships between the independent authorities and supervisors, both at EU and national levels shall be included.

H. Breach, accidents, and remedies.
The AI-regulation shall identify what is meant for breach and accidents, and the consequent paradigm of controls, sanctions, and remedies in case of defaulting behaviours from the AI controller and his/her delegates.
Considering that the GDPR provides for a series of civil, criminal, and administrative offences in case of infringement of the stated obligations, it appears coherent to identify a graduated and multilevel system of prevention, deterrence, and punishment tools according to the binding nature of some obligations and the (attempted) damage produced to individuals, groups, or collectively with the defaulting behaviours.

[46] Ravaja, N., Harjunen, V., Ahmed, I. et al., 'Feeling Touched: Emotional Modulation of Somatosensory Potentials to Interpersonal Touch' (2017) *Sci Rep* 7, 40504. https://doi.org/10.1038/srep40504.

As far as the liability model is concerned, strict liability or fault-based paradigms suitability have been explored both from authors[47] and policy makers[48]. The article 82 GDPR states any person who has suffered material or non-material damage because of an infringement of the GDPR is entitled to seek compensation, and any controller involved in the data processing shall also be liable. As a consequence of the principle of accountability, to avoid liability, data controllers need to prove that they are not in any way responsible for the event that caused the harm. Some authors argued that as far as liability in the field of AI is concerned, "*gradual layered approach to liability grounded on accountability principles*"[49] including "*reversal of the burden of proof, compulsory insurance, funds, regulatory constraints, criminal sanctions*"[50] tailored to the significant deviation from the required standard of compliance, as it can be assessed by humans only if it refers to their action, otherwise "*the deviation from the standard of conduct by AI is assessable only with the help of 'technologies' with the characteristics required by the accountability principle*"[51]. From this perspective, the *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*[52] confirmed the human-centric perspective aimed at guaranteeing the same protection to individuals for harm caused by AI-based technology as other technologies. The possibility to amend/introduce that ground within the Product Liability Directive has been already envisaged in the mentioned report. Whether this is the final approach adopted by the EU legislative initiative or not, it may be useful to complete the frame with the measures aimed at promoting the exercise of data subject/addressee's rights as well as the enforcement tools in light of the principle of accountability, as suggested by authors, in terms of multi-layered accountable liability.

6. Potentialities of the proposed model in light of extra-EU data protection law initiatives

The proposed model finds a validation in light of the role that GDPR has got on recent extra-EU reforms on data protection law.

[47] Paulius Čerka - Jurgita Grigienė, Gintarė Sirbikytė, 'Liability for damages caused by artificial intelligence' (2015) Computer Law & Security Review, 31, 3, 376-389; Gerhard Wagner, 'Robot Liability', in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, *Liability for Artificial Intelligence and the Internet of Things*, cit., 27 ff. and Ernst Karner, 'Liability for Robotics: Current Rules, Challenges, and the Need for Innovative Concepts', *ibidem*, 117 ff., Erica Palmerini - Andrea Bertolini, 'Liability and Risk Management in Robotics', in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Nomos, 2016), 225 ff.

[48] European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics [2015/2103(INL)].

[49] Giovanni Comandé, *cit.*, 177.

[50] *Ibidem*, 182.

[51] *Ibidem,* 177. See also Sonia K. Katyal, cit., that proposes a system based on culture of accountability for algorithms.

[52] See footnote 27.

In this regard, we observe that a whole chapter of the GDPR is dedicated to personal data transfer to third countries (or international organisations) regulation. The first condition to allow these extra-EU flows is that the EU Commission considers the given foreign data protection legislation as adequate (*i.e.* the adequacy decision issued under article 45 GDPR). This approach enabled a mechanism of compliance harmonization to facilitate personal data flows from (and to) non-EU Member States.

For example, the Turkish Protection of Personal Data entered into force in October 2016. It shares with the GDPR the structure aimed at providing notions, principles, and a governance to frame the legal conditions for data processing[53]. First of all, the Turkish legislation defines what is a data processing and identifies a series of roles within the data processing: Relevant person, Personal Data, Special Personal Data, Person in Charge of Data, Data Processor. Significant principles include lawfulness, purpose limitation, proportionality and measurability of all data processing tools, data retention. Also legal conditions to enable data processing recall articles 6 and 9 GDPR structure, even if categories of data are not distinguished in terms of legal basis of the data processing. Despite of the GDPR, the Turkish system provides a specific and separated regulation for health data processing[54], mainly addressed to health service providers and operators, as well as to data subjects and individuals and entities who provide hardware, software, and file systems for healthcare services, in order to define specific safeguards and constraints for this kind of data.

Analogies with the GDPR structure emerge also from an analysis of the Israeli framework. The data protection system is part of a more general protection of the right to privacy, that is considered an expression of the human dignity[55]. The technological progress that characterizes Israeli infrastructures and services allowed to set a direct bridge between the right to privacy, as recognized by the constitution, and the need to regulate the consequences of its violation under the Privacy Protection Act in 198156 that regulates databases under a series of principles that recall the ones stated in the GDPR. Transparency, purpose limitation, confidentiality ad data security, data integrity, providing a series of rights to the data subjects like the right to access, correction of stored information, deletion, objection, consent withdraw. In addition, in 2017, the Privacy Protection Regulations (security) have been enacted, focusing on data security for data storage[57]. Accordingly, a data govern-

[53] Burcak Unsal, 'Protection of Personal Data in Turkey and Japan' (2016) 2 Turk Com L Rev 187.

[54] Personal Health Data Regulation, https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm.

[55] Basic Law: Human Dignity and Liberty § 7, SH No. 1391, 5752 (Mar. 25, 1992), as amended, see *Soren* Zimmermann, 'The Legal Framework of Data Protection in Israel: A European Perspective' (2019) 5 Eur Data Prot L Rev 246; on the legal strategy see Eldar Haber, Aurelia Tamò-Larrieux (2020), 'Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security', Computer Law & Security Review, 37, 105409.

[56] The Privacy Protection Law, 5741-1981, 35 Laws of The State of Israel [LSI] 136 (5741-1980/81), as amended.

[57] Privacy Protection Regulations (Data Security), 5777-2017 (PPDS), Kovetz Hatakanot [KT] [Subsidiary Legislation] 5777 No. 7809 p. 1022, available on the Ministry of Justice website, http://www.justice.gov.il/, Ruth Levush, Israel: Online Privacy Protection Regulations Adopted, Global Legal Monitor (June 14, 2017),http://www.loc.gov/ law/foreign-news/ article/israel-online-privacy-protection-regulations-adopted/, archived at https://perma.cc/QCU8-TJS3.

ance has been established to identify duties and responsibilities. In particular, a databank owner has to provide an information similar to the one stated in the GDPR. Furthermore, four categories of database are identified with different safeguards considering a predetermined risk-assessment. This basic regime has been integrated by the Supreme Court jurisprudence that interpreted the statutory law in light of the human dignity introducing a more effective data subject-oriented regime. Thanks to these features, Israel has received the adequacy decision in January 2019.

Another legislative initiative inspired by the GDPR is the Brazilian General Data Protection Law (LGPD), Federal Law no. 13.709/2018, that has been enacted in order to provide a comprehensive legal framework on data protection. It will enter into force in 2021, considering the one year postponing due to Covid-19 emergency. In short, GDPR constituted an expressed model as long as notions, principles, and legal basis for data processing are similar to the ones stated for the EU, including the identification of a data protection officer and a data breach policy[58]. The main difference with the GDPR consisted of the lack of a national control entity, like a data protection authority, that indeed has been established in 2019.

The provided examples identified a trend towards a cross-fertilization inducted both by the adequacy decision system, that directly impacts on the compliance activities of any third-party transfer, and by the fact that GDPR constitutes an opportunity to enhance an effective cultural change on data protection in light of the by-design and by-default principles.

The alignment could be more problematic if we consider the Chinese system. Even if the Chinese Cybersecurity law introduced in 2018 has seriously made a step forward towards data subjects' rights, several issues remain open[59]. Main differences emerge, in fact, in light of the possibility to exercise data subjects' rights whereas the data controller is not private[60], justifying monitoring and surveillance activities that, threating the democratic values, prevent EU from opening data flows without the needed technical and organizational safeguards provided under articles 46 GDPR.

These reasons, including the lack of any other specific strategies on AI regulation, support and endorse the proposed "interoperability" of the GDPR-model for further purposes, as

[58] Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018. Fernando Bousso, 'Perspectives of the European General Data Protection Regulation (GDPR) in Brazil' (2018) 2 Int'l J Data Protection Officer, Privacy Officer & Privacy Couns 31.

[59] Sarah Wang Han and Abu Bakar Munir, 'Information Security Technology – Personal Information Security Specification: China's Version of the GDPR' (2018) 4 Eur Data Prot L Rev 535.

[60] In fact, it does not provide strict conditions for data processing and data subjects' consent could be implicit (unless a given provision states that it has to be expressed and explicit). The new regulation addresses specific information obligations, included a set of shared principles (like confidentiality, lawfulness, fairness, transparency, and necessity) that are concretely applied as technical measures to avoid possible data breach. Data subjects' information covers a significant chapter within the new regulation, including the notification of data breach. Jyh-An Lee, 'Hacking into China's Cybersecurity Law', 53 Wake Forest L. Rev. (2018), at 101.

it is already considered as a model to follow to better enhance fundamental rights protection within different systems.

7. Conclusive remarks

This paper aimed at discussing some key-issues emerging from the debate on possible AI regulation initiatives, highlighting how the GDPR – at this stage mainly assumed to cover the lawfulness pillar – shall be taken into consideration as a model of law-making under its structure and approach.

However, contents for AI-systems shall be extended to the entire challenges that the processing – also of non-personal data – of a huge amount without human control of the results launches.

Current works issued by policy making on the EU Commission strategy on AI are addressed to promote a risk-based and human-centric approach, strengthening the role of interdisciplinary skills and competence to serve the new paradigm.

Our contribution to shape the new cultural approach to face the societal and technological challenges within the "big data processing era" proposes, indeed, the development of a legal paradigm able to develop a multilevel system of compliance for AI-based technologies on shared principles and a predetermined suggested governance to allocate roles and responsibilities in every relevant step of the AI-process development, identifying possible follow-up mechanisms that must be supported not only by the stakeholders and economic operators, but also by institutions.

Within these terms, the GDPR still recalls the synecdoche literary figure of speech, not only because it is a part of the lawfulness compliance of an AI-system that processes personal data, but because it stands for a larger efficient risk-based model, built up on compliance by design and by default principles, that is suitable to be replicated to regulate a more comprehensive accountable use of the Artificial Intelligence techniques.